Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Testimony of Susan Grant
Director of Consumer Protection
Consumer Federation of America
Before the House Committee on Energy and Commerce
Subcommittee on Commerce, Trade and Consumer Protection
December 2, 2010

"Do-Not-Track" Legislation: Is Now the Right Time?

On behalf of Consumer Federation of America, an association of nearly 300 nonprofit consumer organizations in the United States that was established in 1968 to advance the consumer interest through research, advocacy, and education, I am pleased to submit testimony on this important question: is now the right time for "do-not-track" legislation. The answer, simply put, is Yes.

As a recent Wall Street Journal investigative series[1] so clearly detailed, consumers are being tracked on the Internet wherever they go, whatever they do, without their knowledge and consent. Information about their online activities – what they search for, what they click on, what they purchase, what they share with others – is compiled, analyzed, and used to profile them. Sometimes information that is gathered about them offline is added to create even richer profiles. This "behavioral tracking" is primarily used for marketing purposes at this point, but it can also be used to make assumptions about people in connection with employment, housing, insurance, and financial services; for purposes of lawsuits against individuals; and for government surveillance. There are no limits to what types of information can be collected, how long it can be retained, with whom it can be shared, or how it can be used. As the Wall Street Journal characterized it in the beginning of its series, "one of the fastest-growing businesses on the Internet is the business of spying on consumers."[2]

If someone were following you around in the physical world – tailing you and making note of everywhere you go, what you read, what you eat, who you see, what music you listen to, what you buy, what you watch – you might find this disturbing. The argument that: "We don't know your name, just the make and model of your car, and we're only going to use this information to send ads to you," might not assuage your concerns about being stalked. On the Internet, even if the tracker doesn't know your name, you are not anonymous. As the Federal Trade Commission[3] and members of Congress[4] have

[1] Wall Street Journal, *What They Know*, series of articles from July 31-August 10, 2010, http://online.wsj.com/public/page/what-they-know-digital-privacy.html
[2] Julia Angwin, *The Web's New Gold Mine: Your Secrets*, Wall Street Journal, July 31-August 2, 2010
[3] FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising, 21-25, February 2009 www.ftc.gov/os/2009/02/PO85400behavadreport.pdf

recognized, your Internet Protocol address and other unique persistent identifiers are essentially personally identifying information.

And as the Wall Street Journal put it, the skill of data handlers "is transforming the Internet into a place where people are becoming anonymous in name only."[5] The ability to cross-reference data makes it easy to make assumptions about people and treat them a certain way based on information that has been collected about their activities, even if you don't know their names. Furthermore, as news reports and scholarly articles have described, it is relatively easy to re-identify data that is supposedly anonymous.[6]

With more and more people using the Internet as an essential tool for communications, education, managing their finances, researching health and other sensitive subjects, buying goods and services, sharing information through social networks, engaging in political and civic discourse, accessing government programs and benefits, and storing personal and workplace documents, it is crucial that they be able to exert effective control of the collection and use of information that is gleaned from their online activities. No matter what one thinks about the benefits and risks of online tracking – and there are many differing views on the subject – the fact is that individuals have a basic right to privacy and this right must be respected. As the United Nations stated in The Universal Declaration of Human Rights, which was adopted more than six decades ago:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks.[7]

In many respects, our "home" is now the Internet, and much of our correspondence is now online, but our basic right to privacy remains unchanged. Congress recognized the fundamental importance of consumers' privacy in the context of marketing when it enacted the Telephone Consumer Protection Act[8] and the Telemarketing and Consumer Fraud and Abuse Prevention Act,[9] which limited the times of day that telemarketing calls could be made and restricted other telemarketing practices, and gave the Federal Trade Commission the authority to promulgate rules governing telemarketing. In 2003 when the FTC amended the Telemarketing Sales Rule[10] to create the national "do-not-call" registry, the agency

---

[4] See discussion draft of privacy bill by Representative Rick Boucher (D-VA) and H.R. 5777 introduced by Representative Bobby Rush (D-IL), both of which define "covered information" to include any unique persistent identifiers including IP address.

[5] Emily Steel and Julia Angwin, *On The Web's Cutting Edge, Anonymity in Name Only*, Wall Street Journal, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html

[6] See Nate Anderson, *"Anonymized" data really isn't – and here's why not*, last updated September 8, 2009, http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars; Arvind Naryanan and Vitaly Shmatikov, *Myths and Fallacies of "Personally Identifiable Information,"* Communications of the ACM, June 2010, Vol. 53, No. 6, http://www.cs.utexas.edu/~shmat/shmat_cacm10.pdf; Michael Barbaro and Tom Zeller, Jr., *A Face is Exposed for AOL Searcher No. 4417749*, New York Times, August 9, 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=2&ex=1312776000&pagewanted=all

[7] Article 12, *The Universal Declaration of Human Rights*, December 10, 1948, http://www.un.org/en/documents/udhr/index.shtml

[8] 47 U.S.C. § 277 *et seq*.

[9] 15 U.S.C. §§6101-6108

[10] 16 CFR Part 310

acknowledged that the company-specific approach, which obliged consumers to inform each company one-by-one that they did not want to receive telemarketing calls, was "seriously inadequate to protect consumers' privacy from an abusive pattern of calls from a seller or telemarketer" and that consumers were "angered and frustrated" by the pattern of unsolicited calls they were receiving.[11] The FTC also said that industry self-regulatory programs such as the Direct Marketing Association's Telephone Preference Service fell short because they were voluntary and, "to the extent that sanctions exist for non-compliance, DMA may apply those sanctions only against its members, not non-members."[12] The national "do-not-call" registry provides consumers who do not want to receive telemarketing calls with an easy-to-use mechanism to opt-out, and just as importantly, telemarketers are legally obliged to honor their opt-out decisions. Now is the time to create an easy-to-use mechanism to enable consumers to opt-out of online tracking if they wish to do so, and a legal requirement to honor their decisions.

While online tracking is less visible to consumers than being interrupted at dinner by telemarketing calls, Americans in large numbers are clearly concerned about this practice. A 2008 poll by Consumer Reports National Research Center showed that 72 percent were concerned about their online activities being tracked and profiled by companies. Fifty-three percent were uncomfortable with Internet companies using their email content or browsing history to send them relevant ads, and 54 percent were uncomfortable with third parties collecting information about their online behavior. Ninety-three percent thought that Internet companies should always ask for permission before using personal information and 72 percent wanted the right to opt out when companies track their online behavior.[13]

A 2009 survey by researchers at the University of Pennsylvania and the University of California found that 66 percent of respondents did not want the Web sites they visit to show them ads tailored to their interest, and when the common tracking methods were explained, an even higher number rejected tailored advertising. For instance, 84 percent said No to tailored advertising if it was based on following them on *other* Web sites they had visited. More than 90 percent agree that there should be a law that requires Web sites and advertising companies to delete all stored information about an individual if the person requests them to do so, and 63 percent believe that advertisers should be required by law to immediately delete information about their Internet activities.[14] More recently, a poll commissioned by the nonprofit organization Consumer Watchdog in July 2010 revealed that 90 percent of Americans wanted more laws to protect privacy, 86 percent favored the creation of an "anonymous button" that allows individuals to stop anyone from tracking their online searches or purchases, and 80 percent wanted a "do-not-track-me" list for online companies that would be administered by the FTC.

CFA and other consumer and privacy organizations first called for creating a "do-not-track" mechanism in joint comments to the Federal Trade Commission in 2007 in connection with an FTC Town Hall on "Ehavioral Advertising: Tracking, Targeting, and Technology."[15] We proposed it as one of several pro-active steps that the FTC should take in order to protect consumers as behavioral tracking becomes more ubiquitous.

---

[11] Federal Register Vol. 68 No. 19, January 29, 2003, p. 4631
[12] *Id*
[13] Consumers Union news release, September 25, 2008, http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html
[14] Turow et al, *Americans Reject Tailored Advertising*, http://repository.upenn.edu/asc_papers/137/
[15] http://www.consumerfed.org/elements/www.consumerfed.org/file/other/FTC_sign-on_letter_Ehavioral_Advertising.pdf, November 1, 2007

In 2008, in response to the FTC's proposed principles for online behavioral advertising, CFA submitted comments with Consumers Union urging stronger action, including creating a "do-not-track" mechanism.[16] We argued that self-regulatory programs such as such as the National Advertising Initiative[17] fail to provide consumers with an effective means of opting out of online tracking because consumers are not aware of them, there is no requirement that companies participate in them, there is no oversight or transparency, and there is no enforcement. Furthermore, we noted that the opt-out mechanisms that these voluntary programs provide to consumers, which are based on cookies, did not work for some tracking methods and fail to provide persistent protection from unwanted tracking since cookies may be deleted for a variety of reasons.

In July of 2009, a consortium of four trade associations proposed new voluntary principles[18] for behavioral advertising and promised to implement a self-regulatory program in early 2010. It's late in starting, but, as a New York Times blog post pointed out, the proposal largely codified the practices that companies were already engaging in and failed to endorse ideas that "might give users more meaningful information and control over how their behavior is being tracked."[19] One of those ideas is a browser-based mechanism for avoiding tracking, which I will discuss in more detail later.

The consortium's principles fall short of what we would like to see, even given the inherent limitations of voluntary initiatives, in several respects. For instance, they apply to tracking for advertising but not for other purposes. They do not apply to tracking by the Web site that the consumer is visiting if the site intends to use that information itself or to share it with its affiliates. No notice or choice is required for first party tracking and use and or for affiliate sharing. This is predicated on two false assumptions. The first is that consumers are not troubled by their activities on a Web site being tracked and used by the owner of the site for whatever internal purpose it wishes. The second is that consumers would know who the Web site's affiliates are and would have no objection to the information about their activities on the site being shared with affiliates.

Under these voluntary principles, Web sites could allow third parties to track consumers that visit them, without obtaining any consent from consumers. Those third parties would have to give notice and a "choice" mechanism, which since it does not have to be "opt-In" would undoubtedly be "opt-out."[20] But there are several different options for how the notice and choice could be presented to consumers and how they would exercise their choices. The principles also provide for the possibility of multiple self-regulatory programs that would manage centralized choice mechanisms for member companies that wish to use them. The principles and the systems they would put in place are complicated and confusing, and since the choice mechanisms would probably be cookie-based, they will not work with some tracking methods and they won't be persistent. Furthermore, though many companies will voluntarily sign up, not all will, and the enforcement powers of self-regulatory programs are limited to admonishing and expelling members.

---

[16] http://www.consumerfed.org/pdfs/CFA-CU-behavioralmarketingcomments.pdf, April 11, 2008

[17] See World Privacy Forum report, *National Advertising Initiative: Failing at Consumer Protection and at Self Regulation*, November 2007, http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf.

[18] www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-070209

[19] See Saul Hansell, *Four Privacy Protections that the Online Ad Industry Left Out*, July 6, 2009, http://bits.blogs.nytimes.com/2009/07/06/four-privacy-protections-the-ad-industry-left-out/?pagemode=print

[20] Only Internet Service Providers and others that collect all or nearly all of consumers' Web traffic would be required to obtain opt-ins; opt-ins are also required under this self-regulatory program for collection and use of "sensitive" information, but that is too narrowly defined to offer adequate privacy protection.

In September 2009 CFA and several other consumer and privacy groups released a Legislative Primer for Online Behavioral Tracking and Targeting,[21] which outlines the key elements that we believe are necessary to protect consumers. Once more, we called for a "do-not-track" mechanism. We are pleased that now this idea is finally starting to get the careful consideration that it deserves.

Our thinking about what this mechanism would be and how it would work has evolved over time. It would not operate in the same way that the national "do-not-call" registry does – there would be no need for consumers to provide their IP addresses or other personal information to a database, and therefore no cause for concern about the security of that information. It would not operate using cookies, one reason why the NAI approach has been a failure, since cookies are not always persistent and do not work with some tracking methods.

As we envision it, the "do-not-track" mechanism would be a setting in Web browsers that consumers could use to indicate that they do not wish to be tracked. The browsers would express the consumers' preferences to the Web sites they visit. I am not a technologist but am fortunate to have colleagues in organizations such as the Electronic Frontier Foundation who explain that this mechanism would be simple for both consumers and trackers to use. It is easy to implement as an add-on; it is already being used as an add-on to the Mozilla Firefox browser,[22] and it would be easy to implement for Web services. As consumers whose numbers are on the national "do-not-call" registry can opt-in to receiving calls from telemarketers on a company-by-company basis, so could consumers give permission for tracking by certain entities, in this case through their browser settings.[23]

The FTC would not dictate the design of the technology but would set the overall goals that it should accomplish: providing consumers with a simple, easy-to-use mechanism that effectively and persistently enables them to exert control over online tracking. All browsers would be required to include a "do-not-track" mechanism as a standard feature, at no extra cost to consumers. And just as important, all trackers would be required to honor the consumers' preferences.

Industry members would need to work together, as they often do in implementing technologies that must be interoperable, to ensure that these mechanisms work as intended. The FTC should be required to perform audits and "mystery browsing" to ensure that trackers are indeed complying with consumers' requests, since it is very difficult for consumers themselves to know if their information is being tracked and how it is being used.

We have heard dire predictions that "do-not-track" will destroy the Internet and kill jobs. We heard the same predictions about the national "do-not-call" registry but, as an Associated Press article noted a year after it was launched, the sky did not fall and telemarketing survived.[24] Obviously, not all consumers will use a "do-not-track" mechanism, and some may decide to allow tracking by specific

---

[21] http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf, September 1, 2009

[22] See Christopher Soghoian & Sid Stamm, *Universal Behavioral Advertising Opt-out*, https://addons.mozilla.org/en-US/firefox/addon/12765.

[23] See Arvind Narayanan, "*Do Not Track" Explained*, September 20, 2010, http://33bits.org/2010/09/20/do-not-track-explained/ and http://donottrack.us/, a website created by Mr. Narayanan, Jonathan Mayer and other researchers that provides information about how this "do-not-track" concept would work.

[24] *Telemarketing Firms Surviving "Do Not Call,"* LA Times, October 18, 2004, http://articles.latimes.com/2004/oct/18/business/fi-telemarketers18

entities but not others. Other means of advertising, such as contextual advertising, where ads are served based on what the consumer is looking at on a site at that time, will be unaffected. It is also important to note that serving ads to consumers is only one way that they find products and services they want online. They use search engines, Web sites that provide comparative information about products and services, recommendations from people they know, online auction sites, and other means to find what they need on the Internet. It would be a sorry state of affairs if the only way that ecommerce could survive is by spying on consumers to guess what they want.

We have other concerns about online tracking that will not be eliminated by creating a "do-not-track" mechanism. For example, we believe that there are some types of sensitive information, such as that related to health conditions or sexual preference that should not be tracked at all. We also believe that some uses of behavioral profiles created by tracking, such as for employment, insurance, housing or financial services, should not be allowed. First, the assumptions made about consumers based on their Web activities are not necessarily accurate. This may not matter much, at least to consumers, if it results in advertisements for pickup trucks being sent to people who would prefer sedans. But if these profiles are used to make inaccurate assumptions about people for purposes of credit, employment or insurance, it does matter.[25] Second, it is inherently unfair to follow consumers around the Internet to make decisions about them based on activities that may be totally unrelated to the job, product or service in question.

I may be searching online for information about cancer or HIV because a friend or relative is ill; I certainly would not want my insurance company to know about my searches or to make any determinations about me on the assumption that I have that condition. And I don't think that anyone here would be comfortable with creditors using who your friends are in social networking sites and what you chat about as a factor for determining what kind of credit offer to make to you.[26] This is already happening, and Congress should act to stop it.

We also believe that there must be limits to the length of time that this data can be maintained, that consumers should have the right to see, correct and delete such data, and that access by the government or others for purposes beyond advertising should be limited.

Creating a "do-not-track" mechanism, while not a substitute for comprehensive privacy protection, could nonetheless help ameliorate these concerns. To the extent that consumers have real, effective control over information about their online activities, they can prevent that information from being collected and used in ways that they may find objectionable.

Thank you for holding this hearing to explore the need for a "do-not-track" mechanism. I hope that this will lead to legislation in the near future. We will be happy to provide any additional information that may be needed and to support "do-not-track" legislation.

---

[25] See Emily Steel and Julia Angwin, *On The Web's Cutting Edge, Anonymity in Name Only*, Wall Street Journal, August 4, 2010, http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html, for a description of how online behavioral tracking is used to make assumptions about consumers to serve different credit card offers to them.

[26] See *Social networking: Your key to easy credit?* Erica Sandberg, http://www.creditcards.com/credit-card-news/social-networking-social-graphs-credit-1282.php.